Hewlett Packard
Enterprise

HPE Security ArcSight ESM

Software Version: 6.11.0

Release Notes

April 12, 2017

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2017 Hewlett Packard Enterprise Development, LP

Follow this link to see a complete statement of copyrights and acknowledgements: https://www.protect724.hpe.com/docs/DOC-13026

Support

Contact Information

Phone	A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hpe.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

Welcome to ESM 6.11.0

ArcSight Enterprise Security Management (ESM) is a comprehensive software solution that combines traditional security event monitoring with network intelligence, context correlation, anomaly detection, historical analysis tools, and automated remediation. ESM is a multi-level solution that provides tools for network security analysts, system administrators, and business users.

ESM includes the Correlation Optimized Retention and Retrieval (CORR) Engine, a proprietary data storage and retrieval framework that receives and processes events at high rates, and performs high-speed searches.

What's New in This Release

This topic describes the new features and enhancements added in ESM 6.11.0.

IPv6	**IPv6 Connectivity Support** ArcSight components like the Console, Command Center, Web Service Layer APIs, Forwarding Connector, SmartConnectors (including those hosted on the ArcSight Management Center), and High Availability ESM clusters can communicate with each other using IPv6 communication - both in dual (IPv4/IPv6) and IPv6-only modes.
	IPv6 Data Support Using the latest SmartConnectors supporting both IPv4 and IPv6 and updated parsers, all address fields (for example, Attacker, Source, Target, Destination, and so on) in the ESM schema now display IPv4 or IPv6 address as appropriate. Old SmartConnectors and old parsers will continue to use the deviceCustomIPv6Address fields for IPv6 addresses. Refer to the field mapping information in your *FlexConnector Developer's Guide*.
	Region (Geo) Codes The region code standard is now based on ISO 3166-2. This standard includes support for IPv4 and IPv6 addresses. Not all IPv6 addresses are mapped to a region code. See the topic, "Geographical Attributes," in the *ArcSight Console User's Guide*.
	Zones For accurate asset modeling, system-supplied zones have been updated to include IPv6 addresses. In the ArcSight Console, you now have `/All Zones/ArcSight System IPv6`. This category has its own list of addresses for Dark Address Space, Private Address Space, and Public Address Space Zones specific to IPv6 addresses. The existing `/All Zones/ArcSight System` continues to include IPv4 addresses. See the topic, "Modeling the Network," in the *ArcSight Console User's Guide*.

ArcSight Command Center Enhancements

Dashboard Navigator

The Dashboard Navigator has been enhanced to provide a streamlined view of dashboards, with navigation similar to that of active channels. See the topic "Managing Dashboards in the Dashboard Navigator Page" in the *Arcsight Command Center User's Guide* for details.

Query Viewers

Previously, only query viewers in tabular format were available on the Command Center dashboard page. Now, query viewers in chart format are also available.

See the *ArcSight Command Center User's Guide* for more information about this feature.

Data Monitor Enhancement on the Dashboard and Dashboard Navigator

All data monitor types are now available in the Command Center. Note that the geographical graph is now available.

See to the *ArcSight Command Center User's Guide* for more information about this feature.

Event Graph Enhancement Dashboard Navigator page - Topology Graph

A variation of the Event Graph that displays event endpoints in relation to each other, in terms of Source Nodes, Event Nodes, and Target Nodes. This graph allows you to explore the relationships and connections among the nodes. Hover over a node to highlight that node's connections. Click individual nodes to drill down and explore the relationships among the nodes.

See the *ArcSight Command Center User's Guide* for more information about this feature.

Field Summary Address Fields Are Now Strings

Previously, all Field Summary address fields were treated as numbers; these fields are now treated as strings to accommodate IPv6 addresses.

Save Dashlets as CSV Files

You can now save dashlets as CSV files. See the topic, "Downloading a Dashlet to a CSV File" in the *ArcSight Command Center User's Guide*.

Dark Theme

The Command Center now provides the ability to switch the web interface to a dark theme. The dark theme reduces glare from the screen, therefore providing visual comfort in dark room environments.

Refer to the topic, "Basic Navigation" in the *ArcSight Command Center User's Guide*.

Navigate from a Dashboard to a Channel

You can now drilldown directly to a channel, view that channel, and save it as a resource.

Refer to the topic, "Navigate from a Dashboard to a Channel" in the *ArcSight Command Center User's Guide*.

Access Integration Commands from an Event List

You can now access Integration Commands directly from event links in an Active Channel Event List.

Refer to the topic, "Accessing Integration Commands from an Event List" in the *ArcSight Command Center User's Guide*.

Access ArcSight Investigate from an Event List

You can now access ArcSight Investigate directly from four areas of the ArcSight Command Center interface. These access options are enabled on the Command Center user interface if ESM is configured to integrate with ArcSight Investigate, and are available in:

- Event links in an Active Channel Event List. The commands available are:
    - `ArcSight Investigate`
    - `ArcSight Investigate (Multiple Fields)`
- Event Details, for supported ArcSight Investigate fields. The commands available are:
    - `ArcSight Investigate`
    - `ArcSight Investigate (Multiple Fields)`
- Event Visualization; click to access `ArcSight Investigate` for supported ArcSight Investigate fields.
- Dashboards; click to access `ArcSight Investigate` for supported ArcSight Investigate fields.

Additionally, there is a new integration command in `/All Integration Commands/ArcSight Administration/ArcSight Investigate`. With this integration command, you have two options:

- By Source and Destination
- By Vendor and Product

Refer to the topic, "Accessing ArcSight Investigate from an Event List" in the *ArcSight Command Center User's Guide*.

Case Descriptions in a Separate Dialog

Case descriptions now display in a separate, fully controllable dialog window so you can read the entire case description.

Refer to the chapter, "Cases" in the *ArcSight Command Center User's Guide* for details on cases.

Storage Group - Ability to Manually Add Connectors

The Command Center now allows you to manually add a connector that you specify using the connector ID provided through the Event Broker when you add a Storage Mapping.

Refer to the topic, "Adding a Storage Mapping" in the *ArcSight Command Center User's Guide*.

ArcSight Console Enhancements

Dark Theme

The Console now provides the ability to switch the graphical interface to a dark theme. The dark theme reduces glare from the screen, therefore providing visual comfort in dark room environments.

Refer to the topic, "Changing the Console Display" in the *ArcSight Console User's Guide*.

Advanced Selector for a Resource Attribute

Some resources need a resource attribute. For example, a query viewer needs a query to get data from the database. The Advanced Selector button on source resources' Edit panel provides the option to search, then select the resource.

Refer to the topic, "Using the Advanced Selector While Editing Resources" in the *ArcSight Console User's Guide*.

Recents and Favorites in Navigator Panel

For active channels, actors, assets, and cases, the resource Navigator panel now includes two panels: Recents and Favorites. The Recents list is automatically populated, and you add resources to Favorites.

Refer to the topic, "Creating Shortcuts for Resources" in the *ArcSight Console User's Guide*.

Integration with ArcSight Investigate

- `ArcSight Investigate`
- `ArcSight Investigate (Multiple Fields)`

These options are enabled on the Console UI's active channel or the event details' Inspect/Edit panel if ESM is configured to integrate with ArcSight Investigate.

On the Console, the existing `Investigate` option associated with a specific event on an active channel is now renamed **Analyze in Channel**.

Additionally, there is a new integration command in `/All Integration Commands/ArcSight Administration/ArcSight Investigate`

- "Running ArcSight Investigate Searches" to run from an active channel or from the event details' Inspect/Edit panel.
- "Using the ArcSight Investigate Integration Commands" to define target parameters and search by source and destination, or by vendor and product.

Refer to the *ArcSight Investigate User's Guide* for general information about ArcSight Investigate.

Field-Based Active and Session Lists

The **Address** data type was enhanced to support an IPv4 or IPv6 address value. IPv6 addresses are presented in simplified format, if applicable.

A new data type, **MAC address**, is added for MAC address values.

Refer to the topic, "List Authoring" in the *ArcSight Console User's Guide*.

Integration Commands

The following network tools have been added to support IPv6:

- `NsLookup-IPv6 (Linux)`
- `Ping6 (Linux)`

The legacy `NsLookup (Linux)` and `Ping (Linux)` commands are still available for IPv4 addresses. The legacy `NsLookup (Windows)` and `Ping (Windows)` will ping both IPv4 and IPv6 nodes.

Refer to the topic, "Network Tools as Integration Commands" in the *ArcSight Console User's Guide*.

New Variable Functions

The following function is introduced in this release:

`RoundN`

This function takes a double and rounds it off to the specified number of decimal places, from 0 to 5. Use `RoundN` to make long decimal numbers more readable on the Viewer or on reports, for example.

Variable Functions Enhancements

The following functions are enhanced to accept either an IPv4 or IPv6 address as input. These include:

- `ParseIPAddress`
- `ConvertAddressToString`
- `ConvertStringToIPAddress`

The old `ConvertStringToIPv6Address` is now removed from Type Conversion functions.

Refer to the topics, "IP Address Functions" and "Type Conversion Functions" in the *ArcSight Console User's Guide*.

Integration with ArcSight Investigate

You can run searches on ArcSight Investigate from the ArcSight Console and ArcSight Command Center.

See "ArcSight Command Center Enhancements" on page 7 and "ArcSight Console Enhancements" on the previous page for descriptions.

MSSP Reports on EPS Consumption

Two reports (one monthly and one daily) that track EPS (events per second) consumption per customer (tenant) are now available from the ArcSight Marketplace at

https://marketplace.saas.hpe.com/arcsight

These reports are specifically for our managed security service providers (MSSP) partners.

For details, refer to the topic, "Using MSSP Reports" in the MSSP Best Practices document in Protect724.

High Availability Primary Manager as Source of Forwarded Events

In the previous release, the primary ArcSight Manager in a High Availability ESM cluster could only be the destination of forwarded events. In ESM 6.11.0, the primary Manager can now be the source of events, and the forwarding function is picked up by the secondary Manager during a failover.

Refer to the *Forwarding Connector Configuration Guide* for instructions to install and configure the Forwarding Connector on the primary Manager to enable event forwarding from the High Availability ESM cluster.

Web Service Layer APIs

The following fields have been added to support IPv6 addresses:

- `addressAsBytes`
- `translatedAddressAsBytes`

The legacy `address` and `translatedAddress` fields are still available for backward compatibility.

Refer to the topics, "Overview of Changes" in the *ArcSight ESM Service Layer Developer's Guide* for descriptions and examples.

Enable Scaling for Bytes In and Bytes Out Event Fields

A server property is introduced in this release:

```
bytesInBytesOut.scaling.divider
```

The property is set to 1 by default. If this value is set to be greater than 1, the values for Bytes In and Bytes Out event fields are scaled, and are saved in ESM in the scaled units.

Refer to the following topics in the *ESM Administrator's Guide* for more details:

- "Enabling Scaling for Bytes In and Bytes Out Event Fields"
- "Managing and Changing Properties File Settings"

	Forwarding Connector The Forwarding Connector bundled with ESM6.11.0 has the ability to forward events containing IPv4 or IPv6 addresses. If the destination is ESM6.11.0, the IPv6 addresses are forwarded to the address fields (for example, Attacker, Source, Target, Destination, and so on). If the destination ESM's version is earlier than ESM6.11.0, then the IPv6 addresses are forwarded to deviceCustomIPv6Address fields 1- 4. Refer to the *ArcSight Fowarding Connector Configuration Guide* for detailed information on forwarding events to destinations.
	Event Broker ESM can now be a destination for ArcSight Event Broker 2.0. The destination configuration is done with SmartConnectors, followed by Manager integration done during ESM installation or Manager setup. Refer to the *HPE Security ArcSight Data Platform Event Broker Administrator's Guide* for deployment details. ESM provides data monitors and audit events to monitor Event Broker connectivity and forwarding status. Refer to the following topics: • "Consuming Events from Event Broker" in the *ArcSight Console User's Guide* • "Event Broker Monitoring" in the *ArcSight Administration and ArcSight System Standard Content Guide* See also the ESM 6.11.0 Support Matrix for compatible versions.
Bouncy Castle	**FIPS Compliance Enhancement** For FIPS compliance, ESM now uses Bouncy Castle Java cryptography, which replaces Mozilla Network Security Services (NSS). Bouncy Castle enables the support of TLS 1.2 in FIPS mode as well as in Default mode. As a result, the commands `runcertutil`, `runmodutil`, and `runpk12util` are replaced with use of `bin/arcsight keytool`. Also, `nssdb` is replaced with keystore files to handle the storage of cryptographic material such as certificates and keys. See the FIPS appendixes in the *ESM Installation Guide* and the *ESM Administrator's Guide* for details.

Verifying the Downloaded Installation Software

HPE provides a digital public key to enable you to verify that the signed software you received is indeed from HPE and has not been manipulated in any way by a third party.

Visit the following site for information and instructions:

https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning

Upgrade Support

Direct upgrade to ESM 6.11.0 is supported from ESM 6.9.1c, with or without Patch 1, Patch 2, or Patch 3. HPE recommends upgrading to the latest supported patch before upgrading to ESM 6.11.0. Refer to the *ESM Upgrade Guide* for more details.

For details on supported platforms, refer to the HPE ArcSight ESM Support Matrix available on Protect 724 (https://www.protect724.hpe.com).

Geographical Information Update

This version of ESM includes an update to the geographical information used in graphic displays. The version is GeoLite2-City_20170201 (ipdataV6.mmdb file).

Vulnerability Updates

This release includes recent vulnerability mappings from the February 2017 Context Update.

Device	Vulnerability Updates
Snort / Sourcefire SEU 2990 updated	Faultline, Bugtraq, CVE, Nessus, MSSB
Cisco Secure IDS S965 updated	CVE
Juniper IDP update 2826 updated	Faultline, Bugtraq, CVE, X-Force, Nessus, MSSB
IBM Security Host Protection for Desktops 3360 updated	Faultline, CVE, X-Force
IBM Security Host Protection for Servers (Unix) 36.110 updated	Faultline, CVE, X-Force
IBM Security Host Protection for Servers (Windows) 3360 updated	Faultline, CVE, X-Force
IBM Proventia Network IPS XPU 36.110 updated	Faultline, CVE, X-Force

Device	Vulnerability Updates
IBM Proventia Network MFS XPU 36.110 updated	Faultline, CVE, X-Force
IBM Proventia Server IPS for Linux technology 36.110 updated	Faultline, CVE, X-Force
IBM RealSecure Server Sensor XPU 36.110 updated	Faultline, CVE, X-Force
McAfee HIPS 7.0/8.0 content version 7440 updated	CVE

Supported Versions for Distributed Searches

Distributed searches are supported from ESM 6.11.0 to the following versions of ESM and Logger peers:

- ESM 6.11.0
- ESM 6.9.1c
- ESM 6.8c
- Logger 6.3
- Logger 6.2 Patch 1

The only version that supports IPv6 connectivity and IPv6 data search is ESM 6.11.0.

For more information about distributed searches, look at the *ArcSight Command Center User's Guide* topic “Searching Peers (Distributed Search).”

Supported Platforms

See the ESM Support Matrix document available on Protect 724 (https://www.protect724.hpe.com/docs/DOC-3210) for details on ESM 6.11.0 platform and browser support.

Supported Languages

These languages are supported by ESM:

- English
- French
- Japanese
- Simplified Chinese
- Traditional Chinese
- Korean
- Russian

Usage Notes

ArcSight Command Center

Changes to the ArcSight Command Center

Some functions were removed from the ArcSight Command Center UI because these functions are covered either through the ArcSight Console or through ArcSight commands.

User Management

In previous releases, the ArcSight Command Center supported the ability to configure users, user groups, and permissions. These options are no longer available on the ArcSight Command Center UI.

Instead, use the ArcSight Console to manage users, user groups, and user group permissions. Refer to the following topics in the *ArcSight Console User's Guide*:

- Managing Users
- Managing Permissions

Connector Management

In previous releases, the ArcSight Command Center supported the ability to configure registered SmartConnectors. This is no longer available on the ArcSight Command Center UI.

Instead, use the ArcSight Console to configure registered SmartConnectors. Refer to the topic, "Managing SmartConnectors" in the *ArcSight Console User's Guide*.

Server Management

In previous releases, the ArcSight Command Center UI provided options to configure the server, which includes, enabling notifications, setting up external mail servers, authentications, license management, Manager heap size configurations, and so on.

You can perform ESM server management tasks through commands like `managersetup`. Refer to the *ESM Administrator's Guide* for information pertaining to server configurations.

Menu Items Inaccessible in ArcSight Command Center Resized Window

For displaying the Command Center, use a monitor that has a width of at least 1450 pixels. This is the minimum width needed to display all of the top-menu items. This minimum width also applies on a larger monitor when reducing the size of the browser window.

Scroll Bar Issues with Google Chrome and Apple

When using the Chrome or Safari browser to use the ArcSight Command Center, scroll bars may appear inside the data grid on the Storage Mapping tab when the page is loaded for the first time. Adding another row eliminates the scroll bars. Subsequently, adding or deleting rows works as expected.

To avoid this issue, use either Internet Explorer or Firefox.

Viewing Search Results in a Chart on ArcSight Command Center

If you are not getting search results in a chart on the ArcSight Command Center, you need the Adobe Flash Player plugin on your browser. This issue was found in the following browsers:

- Firefox ESR 45.7.0 on RHEL and Windows 2012 R2
- IE 11 on Windows 2012 R2

ArcSight Console

ArcSight Console Dark Theme on Windows

On the ArcSight Console, you can switch from the default daylight theme to dark theme. The dark theme is to reduce glare if you are using the Console in a dark room environment.

Windows Classic theme is not supported for the dark theme on ArcSight Console. For Windows, use the Basic theme.

For general instructions on how to switch from default to dark theme on the Console, see the topic "Changing the Console Display" in the *ArcSight Console User's Guide*.

Events from Event Broker

If you are viewing events on an active channel, you can double-click a specific event to get more event details from the Event Inspector.

One of the details you can select on Event Inspector is Agent ID. If you click Agent ID, you may get the following message:

```
Unable to load resource as this event was likely consumed via Event Broker
```

This is expected behavior. There is no associated resource for events consumed from Event Broker.

Using Windows 10

The ArcSight Console for ESM 6.11.0 is supported on Windows 10. The recommended processors for Windows 10 are either Intel Xeon x5670 or Intel Core i7.

For ArcSight Console in Windows 10, use Internet Explorer as your preferred browser. This preference is set during Console installation time; or after Console installation using the User Preferences setting for Program Preferences.

See also "Using the Edge Browser" below for related information.

Using the Edge Browser

- The ArcSight Console Help does not support Edge as the preferred browser. See also "Using Windows 10" above for related information.
- The Tools command does not work with the Edge browser due to a certificate issue.
- On the ArcSight Console and ArcSight Command Center, viewing PDF reports on the Edge browser is not supported. Either view the PDF report in Internet Explorer, or output the report in HTML format.

Resource Validation

Resource validators for IP and MAC address data have been tightened. After an upgrade, any resources containing incorrect IP addresses or address ranges will be invalidated. The same goes for non-unique MAC addresses. You need to rebuild the invalidated resource with the correct address formats.

You should also look at ESM packages created in previous releases, which may contain assets with the wrong address formats. These can be fixed after importing into this release.

For information on supported IP address range formats, refer to the *ArcSight Console User's Guide*'s topic on "IP Address Ranges."

ESM and Logger Connectivity

ESM in dual stack mode, preferred IPv4/IPv6 will connect with Logger 6.3 or earlier releases. ESM in pure IPv6 mode will not connect with Logger 6.3 or earlier releases.

Configuring Emails for Transport Layer Security

Starting in ESM 6.11.0 there is a server property (`email.tls.desired`) for SMTP servers configured to use Transport Layer Security (TLS).

If your SMTP server is configured to use TLS, you do not need to do anything because, by default, this property is set to `true`.

If your SMTP server is not set to use TLS, then add the property `email.tls.desired=false` to the `sever.properties` file. See the topic, "Managing and Changing Properties File Settings" in the *ESM Administrator's Guide* for information on editing the server.properties file.

If the TLS configurations do not match:

- SMTP server uses TLS and `email.tls.desired=false`, emails are sent without TLS.
- SMTP server does not useTLS and `email.tls.desired=true`, emails are not sent.

If emails fail for any reason, they are not resent.

SSL Client Authentication After Upgrading to ESM 6.11.0

This is applies to those who are upgrading to ESM 6.11.0 from ESM 6.9.1 (no patches) with SSL Client Authentication, and you have used keytoolgui to generate the keypairs and certificates. After upgrading to ESM 6.11.0, re-generate the certificates before you re-start services.

Note: In FIPS mode, you cannot use the keytoolgui. Refer to the *ESM Administrator's Guide* for instructions on regenerating keypairs and certificates.

Actor Model Import Connector

The Actor Model Import Connector for Microsoft Active Directory allows you to develop a model import connector to import actor model data. The Actor Model Import Connector for Microsoft Active Directory to install for ESM 6.11.0 is version 7.5.0.7988.0. This new connector can be configured in a dual stack or pure IPv6 environment. Refer to the *Actor Model Import Connector for Microsoft Active Directory Configuration Guide*.

The old model import connectors can work with ESM 6.11.0 provided those old versions connect to ESM 6.11.0 on dual stack mode using the preferred IPv4 option.

See the ESM Support Matrix document available on the Protect 724 site for details on ESM 6.11.0 supported platforms.

Caution: Install and use the Actor Model Import Connector for Microsoft Active Directory that is provided with the ESM 6.11.0 release. That is the version of the connector that is tested and certified to work with ESM 6.11.0. Do not use previously-supplied versions of the Actor Model Import Connector for Microsoft Active Directory with ESM 6.11.0.

Asset Model Import FlexConnector

The Asset Model Import FlexConnector supports the ability to create and manage the Asset Model within ESM. The Asset Model Import FlexConnector allows you to develop a model import connector to import asset model data from a file. This enables you to create and maintain ESM Network Model data and keep the data in sync with the data in your Asset Management system. The Asset Model Import FlexConnector to install for ESM 6.11.0 is version 7.5.0.7987.0. This new connector can be configured in a dual stack or pure IPv6 environment. Refer to the *Asset Model Import FlexConnector Developer's Guide*.

Earlier Asset Model Import Connector versions enabled the creation of IPv4 assets. This new version enables the creation of both IPv4 and IPv6 assets.

The old model import connectors can work with ESM 6.11.0 provided those old versions connect to ESM 6.11.0 on dual stack, using the preferred IPv4 option.

See the ESM Support Matrix document available on the Protect 724 site for details on 6.11.0 supported platforms.

> **Caution:** Install and use the Asset Model Import FlexConnector that is provided with the ESM 6.11.0 release. That is the version of the connector that is tested and certified to work with ESM 6.11.0. Do not use previously-supplied versions of the Asset Model Import FlexConnector with ESM 6.11.0.

Forwarding Connector

The ArcSight Forwarding Connector can receive events from a source Manager and then send them to a secondary destination Manager, an ArcSight Logger, or a non-ESM destination. The Forwarding Connector to install for ESM 6.11.0 is version 7.5.0.7986.0. Only the Linux executable applies to ESM 6.11.0.

The Forwarding Connector is capable of forwarding events with IPv4 or IPv6 addresses. If the destination ESM supports both IPv4 and IPv6 addresses, then the address fields like Attacker, Source, Target, and so on, will be used. If the destination does not support IPv6 addresses, then the deviceCustomIPv6Address fields 1-4 will be used.

See the ESM Support Matrix document available on the Protect 724 site for details on ESM 6.11.0 supported platforms.

Localization

In some locales, some text strings may not be translated and display in English. These untranslated strings do not affect functionality.

ESM Peer Certification for Content Synchronization

Peering is automatically mutual, so a group of peers may be enabled from a single Manager. Content Management is certified with up to five subscribers, with one additional Manager as a publisher.

> **Caution:** For ESM content synchronization, only ESM peers of the same version are supported. Application of Service Packs, Patches and Hotfixes alter version numbers. You should carefully consider the impact to synchronization during change management.

For information about content management, refer to the following:

- "Creating or Editing Packages" and "Supported Package Resources for Content Synchronization" in the *ArcSight Console User's Guide*
- "Content Management" and "Configuring Peers" in the *ArcSight Command Center User's Guide*

90Meter Cards and Firefox Browser

If you are using Firefox 45.1.1 with 90Meter cards for authentication, you may encounter an error stating that x86\litpkcs11.dll is not supported. If this occurs, contact the 90Meter vendor's support for additional assistance in configuring Firefox to resolve this issue.

> **Caution:** Do not use Firefox 45 and later with Windows 8.1 Enterprise. Use Firefox v38.0.1 ESR instead.

For information on 90Meter cards supported in ESM releases, refer to the ESM 6.11.0 Support Matrix.

Payment Card Industry Data Security Standard (PCI-DSS) Compliance for Peering

For compliance with the Payment Card Industry Data Security Standard (PCI-DSS), use TLS 1.2. Note that all ESM/Logger instances that are peered together must implement ESM 6.11.0 and Logger 6.4 to achieve PCI-DSS compliance. For details on TLS support, see the topic TLS Support in the *ESM Installation Guide*.

Running ArcSight Investigate Searches

ESM 6.11.0 has a set of supported browsers in the ESM Support Matrix (https://www.protect724.hpe.com/docs/DOC-3210). These refer only to browsers for use with the ArcSight Command Center. If you are running ArcSight Investigate 1.0 searches, use only the browsers mentioned in the section "ESM Support of Other ArcSight Products/Components" in the ESM Support Matrix. Locate the line item for ArcSight Investigate 1.0.

General search instructions

- If the search query is on an empty field that is an Integer or Number data type, the query should be of the format

  `<FieldName> = 0,None`

  for example

  sourcePort = 0,None
- When launching ArcSight Investigate integration command, use the default port **443**, unless the port is configured differently.
- If you are a non-administrator user in ArcSight Investigate, you may not be authorized to view certain field values. If you are searching such fields, you will see an `Unknown column` error. If you are a non-administrator user in ArcSight Investigate and you are not authorized to execute a search query, you will see an error that says you are not authorized.
- If you open multiple browser sessions for ArcSight Investigate searches, you will eventually observe slowness in browser response. The threshold is from 5 to 6 sessions. If you open more than that, you should close some browsers.
- ArcSight Investigate search results are case-insensitive. That is by design.

Searching for Attacker Address and Target Address Based on Originator

This information applies to ArcSight Investigate searches executed from the ArcSight Console and from the ArcSight Command Center. The ESM derived fields Attacker Address and Target Address are not found in ArcSight Investigate. Instead, ArcSight Investigate uses the primary fields Source Address and Destination Address.

Assume these values for the following fields:

```
Attacker Address = 1.1.1.1
Target Address = 2.2.2.2
Source Address = 1.1.1.1
Destination Address = 2.2.2.2
```

If the Originator is	And you are searching	ArcSight Investigate returns
Source	Attacker Address 1.1.1.1	sourceAddress = 1.1.1.1
Source	Target Address 2.2.2.2	destinationAddress = 2.2.2.2
Destination	Attacker Address 2.2.2.2	destinationAddress = 2.2.2.2
Destination	Target Address 1.1.1.1	sourceAddress = 1.1.1.1

Searching for Empty Fields

This information applies to ArcSight Investigate searches executed from the ArcSight Console and from the ArcSight Command Center.

If the empty field type in ESM is	Example	Use this search syntax in ArcSight Investigate
String	Name	`Name='', 'None'` **Note:** Use two single quotes without spaces after the equal sign.
Integer or Number	SourcePort	`SourcePort=0, None`

Permissions for searches

- If you are a non-administrator user in ArcSight Investigate, you may not be authorized to view certain field values. If you are searching such fields, you will see an `Unknown column` error.
- If you are a non-administrator user in ArcSight Investigate and you are not authorized to execute a search query, you will see an error that says you are not authorized.

For more information, refer to the *ArcSight Investigate Administrator's Guide*.

Russian characters

Russian characters are not supported in ArcSight Investigate searches. Consult the ArcSight Investigate documentation for updates on this behavior.

Search error due to complex characters

Some field values with complex characters may instruct you to fix the query manually.

When invoking ArcSight Investigate searches from ESM with values that contain both single and double quotes, truncate the value in the ArcSight Investigate Search Input after the second quote symbol. For example, if you ESM value of the Name field is:

```
my_esm_value'with"single'and"double_quotes
```

and it got inserted into Investigate as:

```
Name = 'my_esm_value'with"single'and"double_quotes
```

then truncate it after the single quote:

```
Name= 'my_esm_value'
```

and replace = with `starts with`:

```
Name starts with 'my_esm_value'
```

Supported ESM fields

Below is a list of ESM fields that are supported in ArcSight Investigate searches. For ESM fields that are not on this list, the right-click Investigate options are disabled.

Search error with multiple sessions

When you open multiple search sessions, one after the other, you may eventually encounter the error

```
Fix Error in Query First Unknown Column Name
```

When this happens, close some browser tabs and try again.

List of ESM Fields Supported in ArcSight Investigate Searches

ESM Fieldname
agentAddress
agentDnsDomain
agentHostName
agentMacAddress
agentTranslatedAddress
agentType
agentVersion
applicationProtocol
bytesIn
bytesOut
categoryDeviceGroup
categoryDeviceType
categoryObject
categoryOutcome
categorySignificance
categoryTechnique
destinationAddress
destinationDnsDomain
destinationHostName
destinationMacAddress
destinationNtDomain

List of ESM Fields Supported in ArcSight Investigate Searches, continued

ESM Fieldname
destinationPort
destinationProcessId
destinationProcessName
destinationServiceName
destinationTranslatedAddress
destinationTranslatedPort
destinationUserId
destinationUserName
destinationUserPrivileges
deviceAction
deviceAddress
deviceCustomFloatingPoint1
deviceCustomFloatingPoint2
deviceCustomFloatingPoint3
deviceCustomFloatingPoint4
deviceCustomIPv6Address1
deviceCustomIPv6Address2
deviceCustomIPv6Address3
deviceCustomIPv6Address4
deviceCustomNumber1
deviceCustomNumber2
deviceCustomNumber3
deviceCustomString1
deviceCustomString2
deviceCustomString3
deviceCustomString4
deviceCustomString5
deviceCustomString6
deviceDnsDomain
deviceDomain

List of ESM Fields Supported in ArcSight Investigate Searches, continued

ESM Fieldname
deviceEventCategory
deviceEventClassId
deviceExternalId
deviceFacility
deviceHostName
deviceInboundInterface
deviceMacAddress
deviceNtDomain
deviceOutboundInterface
deviceProcessId
deviceProcessName
deviceProduct
deviceSeverity
deviceTranslatedAddress
deviceVendor
deviceVersion
eventOutcome
fileHash
fileId
fileName
filePath
filePermission
fileSize
fileType
flexNumber1
flexNumber2
flexString1
flexString2
name
oldFileHash

List of ESM Fields Supported in ArcSight Investigate Searches, continued

ESM Fieldname
oldFileId
oldFileName
oldFilePath
oldFilePermission
oldFileSize
oldFileType
requestClientApplication
requestMethod
requestUrl
sourceAddress
sourceDnsDomain
sourceHostName
sourceMacAddress
sourceNtDomain
sourcePort
sourceProcessId
sourceProcessName
sourceServiceName
sourceTranslatedAddress
sourceTranslatedPort
sourceUserId
sourceUserName
sourceUserPrivileges
transportProtocol

Unsupported Features in This Release

The following features are either not supported in this release and no longer available.

- Superindexes
- TRM integration commands from the ArcSight Console

- The NSP device listener as a Destination option in the Forwarding Connector.
- Content sync with older ESM versions is no longer supported.
- The Java Authentication and Authorization Service (JAAS) external authentication mechanism is no longer supported.
- ArcSight IdentityView Solution

The following are not supported in IPv4 and IPv6 environments:

- ESM 6.x Migration Tool, G7 to G9 ESM Express appliance
- ESM 6.x Migration Tool, G8 to G9 ESM Express appliance
- Resource Migration from ESM 5.x
- Event Data Transfer tool to Hadoop systems, including use of Hadoop Connector
- ArcSight Risk Insight
- Reputation Security Monitor (RepSM) 1.5x Solution, including use of RepSM Model Import Connector 7.1.7.7607.0
- Integration with HPE Service Manager, including use of the ArcSM connector
- Threat Central Solution, including use of Threat Central Model Import Connector

Using external authenticators in pure IPv6 environment is not supported

If Active Directory, LDAP, or RADIUS is installed in a pure IPv6 environment, communications are *not* supported with ESM (pure IPv6 or dual stack environment).

However, if Active Directory, LDAP, or Radius is installed in dual stack, communications *are* supported with ESM (pure IPv6 or dual stack).

The following integrations are not supported in a pure IPv6 environment:

- External links to Console Help
- Integration with HPE OM and HPE OMi
- Integration with ArcSight Event Broker 2.0 or ArcSight Investigate 1.0

ESM Integrations:

The following ESM integrations are not supported. If you are using any of the following, *do not upgrade* to ESM 6.11.0:

- Integration with iDefense. Do not run the `idefensesetup` command to launch the iDefense wizard.
- Integration with BMC Remedy, including use of the ArcRemedyClient connector
- Integration with Risk Insight

ESM Service Layer APIs:

- The following deprecated methods have been removed from the ESM Service Layer APIs:
  - public List insertResources(List resources, int relationshipType, R parent) throws ServiceException;
  - public List findAll() throws ServiceException; public boolean containsDirectMemberByName1 (String groupId, String targetId, String name) throws ServiceException;
  - public boolean containsDirectMemberByName(String groupId, String targetId) throws ServiceException;
  - public boolean containsDirectMemberByNameOrAlias1(String groupId, String targetId, String alias, String name) throws ServiceException;

Fixed Issues

The following issues are fixed in this release.

Analytics

Issue	Description
NGS-22558	Running a report with a huge row limit (10,000 rows) in HTML format previously caused the browser to be unresponsive. This is now fixed. The workaround had been to run the report in PDF.
NGS-22274	Previously, pre-persistence rules were triggered when they should not have been. Now, only the events that satisfy the rule condition trigger pre-persistence rules.
NGS-20372	When attempting to save a report that was manually generated, if the report name contained illegal characters such as * " . / : < > ? \ | on Windows and . and / on Linux, so would the filename suggestion. This resulted in an error if it was not changed. Now the filename suggestion changes each invalid character to an underscore.
NGS-20252	Only aggregated fields will be allowed in Group condition of query configuration.
NGS-20143	Using a query with custom parameters which are enumerations within a report resulted in empty output reports being generated. This has been fixed.
NGS-19920	Reports showed Custom Date with $Custom.StartTime variable instead of actual start time, based on a query. This has been fixed in the templates.
NGS-19751	Warnings could occur in the log file indicating that "Trend query took too much time," even if the query was finished before the timeout limit. This issue has been fixed.
NGS-19750	An audit event, report:106, is now generated whenever a report is sent to a recipient successfully. Details pertaining to the status and content of the report, as well as details regarding the recipients, can be viewed with the "Custom Strings" section of the audit event.

Issue	Description
NGS-19749	When a user tried to run an empty report, they would receive an email notification with the report's resource ID in the subject line, and in the message of the email. It was difficult to determine which report was being referenced.<br/> The issue is now fixed. When an email notification is sent regarding an empty report, the name of the report will be displayed in the subject and in the message.
NGS-19748	When a report is generated that is empty or too big, or failed to send, the audit event, report:107, is now created in ESM. If the report size is too big to be sent as an attachment, then additionally the notification will provide the report's URL instead.
NGS-19744	An ambiguous error would occur in the logs where there was a problem with the type of a dependent variable. The error message has been augmented to include more specific information about the error.
NGS-19737	If an Active List has an error adding event data, the resulting log message now includes the Event ID, Device Vendor, Field Name and the schema type.
NGS-19235	When new entries are added to a specific active lists, some of the records (random behavior) can't be deleted. The issue is now fixed.
NGS-19044	When a rule was caught in a loop or firing excessively, the rule would be deactivated and an audit event rule:701 was supposed to be generated, but it was not. An audit event of rule:701 is now generated when a rule is excessive firing or caught in a loop. The issue is now fixed.
NGS-18742	Warnings could occur in the log file indicating that "Trend query took too much time," even if the query was finished before the timeout limit. This issue has been fixed.
NGS-18247	If an Active List had more than 20 columns of type "String" and a user attempted to Apply Settings, ESM would indicate a MySQL syntax error. This issue has been fixed.
NGS-17561	Rule recovery can timeout if there is a high EPS. You can modify the rules.recovery.time-limit property to set a higher recovery time limit to attempt to prevent this timeout so the server will not stop loading events from the database for checkpoint. The default value for rules.recovery.time-limit is 120 seconds (two minutes). However, the timeout can still occur even after you raise the time limit, due to overall system load, high EPS, or a large number of rules. For details on editing the server.properties file, see the "Editing Properties Files" topic in the ESM Administrator's Guide.
NGS-16595	Previously, pre-persistence rules were getting fired/invoked when they should not have been. Now only the events that satisfy the rule condition fire pre-persistence rules.
NGS-15072	When a report is generated that is empty or too big, or failed to send, an audit event is now created in ESM to track the issue.

Issue	Description
NGS-14897	Rules that were disabled by the Rules Engine are now re-enabled automatically on startup.
NGS-14786	When ESM runs with a large number of active lists, long running reports, and trends, the ESM manager would run out of memory after a few days. This issue is now fixed.
NGS-14585	When a string value included a combination of certain special characters such as \ or !, the comparison filter methods StartsWith and Contains would not be able to validate properly. The issue is now fixed.
NGS-14581	When attempting to create an Investigate Channel on a global variable field in an active channel, there would be no result if the user did not have read permission on session lists. This issue is now fixed.

ArcSight Console

Issue	Description
NGS-20632	Filters on URL host names sometimes resulted in unexpected behavior. This issue has been fixed.
NGS-20226	Row height in several tables did not resize when the font was set to a different size. The issue is now fixed.
NGS-20146	When increasing the font size to 20px and 25px on the ArcSight Console, the row height does not auto-resize on the active channel. Row height is now set according to font size in grid view.
NGS-20104	A MAC Address which is not set will now be displayed as empty in the Console.
NGS-19746	When a user was moved to another group and a link was created, and after that selected for deletion, if you did not confirm the deletion in the popup screen and closed the window, the user was deleted anyway. Now, if you close the delete confirmation popup without confirming, the deletion is cancelled.
NGS-19745	The ESM query editor did not maintain the "distinct" parameter when the "order by" section was edited. This issue has been fixed.
NGS-19689	When using SlideShow mode on a multi-screen setup, the second Console could disappear. This issue is now fixed.
NGS-18852	Before ESM 6.8, when using the ArcSight Console to Import and Export Connector Configurations, a user could choose to "Select All" or individually check the box in the "Override" column for the configuration items to import. This functionality has been restored.

Issue	Description
NGS-18270	Event ID column was not visible to the ArcSight Console interface. The visibility of the Event ID column has been enabled.<br/> This issue is now fixed.
NGS-18269	When adding columns using the Customize Columns feature in an active channel, the added columns would appear blank. This issue is now fixed.
NGS-17389	Popup menu shows up on wrong monitor when screen extended vertically. The issue is now fixed. After you extend the monitors vertically then you must restart Console in order the changes to take place.
NGS-17194	When running an Active Channel which has one filter (for example, Destination Address = 198.51.100.0), it works as expected, but when three or more OR conditions of the same kind are added, the same active channel indicates loading, but does not load any events. This is now fixed.
NGS-16582	Previously a SQL&#xA0;query would produce incorrect results under these circumstances: - Running the query via 'arcdt' or - Using an ESM resource that produces a SQL query (for example, Active Channel, Query/Query Viewer, or Report) - The conditions of the SQL query contain some IP address constants - The constants were either by way of 'IN()', or multiple = predicates, and combined by 'OR' operators. This issue has been fixed.
NGS-16111	When increasing the font size to 20px and 25px on the console, the row height did not auto-resize on the active channel. Row height is now set according to the font size in grid view.
NGS-16076	Monitor Events were not included in the replayfilegen utility, resulting in a number of events that was inconsistent with the Active Channel.<br/> This issue is now fixed.
NGS-15682	Searching on Notifications would return no results, because a search for Notifications resources has not been implemented for performance reasons. Therefore searching on that type of resource is disabled. To avoid confusion the dropdown menu for the resource search no longer contains the menu item for Notification.
NGS-14636	When many scheduled reports were running at the same time, an EPS drop could occur.<br/> This issue is now fixed.
NGS-14584	Entries in active lists were considered identical with and without trailing spaces, and deletion of either would result in deletion of both entries.<br/> This issue is now fixed.

Issue	Description
NGS-14289	Filters applied to Connectors would show the filter conditions, rather than the Filter URI.<br/> This issue is now fixed.
NGS-14113	When manually overriding the status in a Last State Data Monitor, some were not visible if large images were used. This has been addressed by adding a scroll bar to the selection window.<br/> This issue is now fixed.
NGS-13673	When multiple recipients were provided in a scheduled report Jobs tab, for example: one user in Email To and one email address in Email Addresses; or two comma-separated email addresses in Email Addresses, then only the first email address in Email Addresses would receive the message. This issue is now fixed.
NGS-13393	Connector's Filter tab is now viewable by users with read-only permissions.
NGS-13390	Previously, the "Last Password Change" date/time value would change to the time of the last login, and passwords never expired. Now, even after restarting the ArcSight Console The "Last Password Change" remains as the date/time when the password was actually changed.
NGS-13085	The ESM query editor did not maintain the "distinct" parameter when the "order by" section was edited. This issue has been fixed.
NGS-11782	The following pop up dialogs will remain on the same screen with Console on Windows: Inline Filter - Condition Editor pop-up dialog Tools - Configure, Results, Nslookup, Ping, PortInfo, Traceroute, and Whois pop-up dialogs
NGS-10765	Event ID column was not visible to the Console interface. The visibility of Event ID column has been enabled. This issue is now fixed.

Issue	Description
NGS-10561	Using a query with custom parameters which are enumerations within a report resulted in empty output reports being generated. This has been fixed.
NGS-9813	Behind the scenes, Manager creates a report in order to export all events from the active channel. Therefore the report must have a report template and a specified filter or filters. For the user to be able to export all events in the active channel, user must have the following permissions: Read access to /All Report Templates/ArcSight System/1 Table/ Read access to the specified event's filter. For example: If a user belongs to a User Group which has in the Edit Access Control Panel, in the Events tab, read access to /All Filters/ArcSight System/Events Types/ArcSight Correlation Events then the user must have read access to /All Filters/ArcSight System/Events Types/ in the Resources tab as well.
NGS-7445	When adding columns using the Customize Columns feature in an active channel, the added columns would appear blank, or missing data.<br/> This issue is now fixed.

ArcSight Manager

Issue	Description
NGS-21835	A data overflow problem was occurring for the fields BytesIn and BytesOut when their values were greater than the maximum value of the integer. The issue is fixed by adding the new integer server property "bytesInBytesOut.scaling.divider" with the default value 1. When the value is set higher than 1, the values received for BytesIn and BytesOut fields are scaled and saved in ESM in the scaled units.
NGS-21776	A new server property "query.concat.null.validation" has been introduced. If enabled, this property applies a validation to concatenation functions used to query data. If all parameters for the function are Null, it will return a Null value as result. Enabling this property might create performance issues if used with very complex filters and large amounts of data. To enable this property, add: query.concat.null.validation=true into config/server.properties and restart ESM Manager for the property to take effect.
NGS-21571	Updating LDAP certificates could result in authorization failures. The updated JRE provided with this release fixes this issue.

Issue	Description
NGS-20938	The following conditions did not always work as filter conditions for an active channel: Event Annotation Stage Name != "Closed" Event Annotation Stage Name != "Incident" The issue is now fixed.
NGS-20521	Annotation information failed to be set correctly when the event was marked as isReviewed. The issue is now fixed.
NGS-20147	It was observed that the case channels were displaying duplication of case data. The bug fix ensures that the duplicate cases do not appear in case channels. The case channels now show one instance of a case that matches a filter as against multiple instances of same case.
NGS-20145	AgentReceiptTime values were showing as epoch timestamps when events were exported from ArcSight Command Center to a CSV file.<br/> This issue has been fixed.
NGS-20144	The informational message "Skipped mac-address mis-match check" was logged as an error. It is now logged at the appropriate level.
NGS-20085	Annotation information failed to be set correctly when the event was marked as isReviewed. The issue is now fixed.
NGS-20037	Sending reports via e-mail fails to attach or embed reports. Use Console and ACC to access report archives.
NGS-19747	Events with timestamps outside a particular range can be adjusted to Manager receipt time or dropped. Use the following settings (with defaults) in the server.properties file to enable this capability: event.time.corrector.enabled (false) event.time.corrector.dropbad (false) event.max.negative.time.offset (default/minimum -1 day) event.max.positive.time.offset (default/minimum +1 day) If the corrector is enabled and event timestamps are within the configured range, no action is taken. If the corrector is enabled and events with timestamps outside the configured range are received, the specified action is taken for those events only, and audit messages are generated. If needed, standard rules can be configured to send notifications when such audit messages are received.
NGS-19496	If you tried to install HA on an unsupported OS version by changing /etc/redhat-release in HA 6.9.1 or earlier a message saying "No package /usr/lib/arcsight/highavail/install/rpms/ERROR/*.rpm available". The error message now indicates that the problem is the wrong OS version.
NGS-19493	ESM ran out of JVM memory in few cases. The issue is now fixed.

Issue	Description
NGS-19222	In order to restrict the maximum number of active channels opened by a user, the property server.channel.maxchannels needs to be set in the server.properties configuration file. Note: changing the property in the console.properties file has no effect. Also note: increasing this parameter leads to a strong possibility of performance degradation, so caution is advised.
NGS-18301	The notification tables stopped being purged when the table got large when a large number of notifications were run. This issue has been fixed.
NGS-18064	During active list import from a CSV file and under certain conditions, date fields would be imported as NULL. This issue is now fixed.
NGS-17969	Events with timestamps outside a particular range can be adjusted to Manager receipt time or dropped. Use the following settings (with defaults) in the server.properties file to enable this capability: event.time.corrector.enabled (false) event.time.corrector.dropbad (false) event.max.negative.time.offset (default/minimum -1 day) event.max.positive.time.offset (default/minimum +1 day) If the corrector is enabled and event timestamps are within the configured range, no action is taken. If the corrector is enabled and events with timestamps outside the configured range are received, the specified action is taken for those events only, and audit messages are generated. If needed, standard rules can be configured to send notifications when such audit messages are received.
NGS-17920	After running reports, the archive report folder name may have leading zero missing in the month number, for instance 2-16-2016. For workaround, customers need to add a property<br/> report.datetime.dateFormat=MM-dd-yyyy<br/> into server.properties and restart the Manager.
NGS-17581	Case channels were displaying multiple rows of case data, one for each event attached to a case. Now duplicate cases do not appear in case channels.
NGS-17553	While running queries, you may have seen a warning in server.log that states "Unexpected:TimeStamp[timestamp]" for example unexpected: Start Time[startTime] Now the query will run successfully.
NGS-17190	The situation reported by the MySQL log message "[ERROR] /opt/arcsight/logger/current/local/mysql/libexec/mysqld: Sort aborted" and the ESM server log message "Temporary sort space limit exceeded" can be addressed by increasing the value of sort_temp_limit in my.cnf.
NGS-16812	In previous releases primary and or secondary hostnames with capital letters would cause various problems in High Availability. This is no longer the case.

Issue	Description
NGS-16701	Users can now adjust the maximum attachment size up to 100 MB for reports that are sent as email attachment, by setting the report.upload.maxFileSize property to the desired size (in MB) in the server.properties file. Refer to the ESM Administrator's Guide to learn how to change the ESM configuration using property files.
NGS-15029	On page manage.jsp, menu RuleEngine section "Loaded Rules" was extended. Table "Loaded Rules" now contains column with total time in nsec and table is ordered by this new column.
NGS-14964	When an Active List had an error, the log message did not have enough detail to help you determine what the error was. These log messages now include the Event ID, Device Vendor, Field Name, and the schema type.
NGS-14927	If you ran an empty report, you would get an email notification with the report's resource ID in the subject line and in the body of the email, making it difficult to determine which report was being referenced. The issue is now fixed. When an email notification is sent regarding an empty report, the name of the report is displayed in the subject and in the message.
NGS-14855	When an archived report was copied from one folder to another folder, then either was deleted, both the original and the copy of the report were deleted. This issue is now fixed.
NGS-14586	In a disaster recovery situation, ambiguous errors would occur if the source and destination machines were set to different timezones. Now, if a timezone mismatch is detected, a useful error message is issued and the operation is aborted.
NGS-14582	When a rule tried to create a case using a filename as part of the case URI or case name, and that filename contained one or more embedded slashes ('/' as in /etc/password), the embedded slashes were conflicting with internal representation causing the filename to be parsed into components. To prevent this misinterpretation, embedded slashes are now replaced with backslashes.<br/> This issue is now fixed.
NGS-14461	When generating Excel reports, the graphs used a Java default number format, ignoring the report's template number format. Now the report's template number format can be used instead of the current Java default number format, by setting the property by setting 'report.chart.value_label.use_template_value_format' to 'true' in the server.properties file.
NGS-14338	The informational message "Skipped mac-address mis-match check" was logged as an error. It is now logged at the appropriate level.
NGS-14130	A new function, RoundN, is introduced in ESM 6.8c Patch 3. You can round a chosen field or variable containing a double number to between 0 and 5 decimal places.
NGS-14056	When a note was added to a resource, a "Note inserted" event was generated but was missing resource information. To address this, the missing information has been added to an audit event.

Issue	Description
NGS-13873	Previously, when importing a package (default) with an active list, the "Last Modified Time" on the active list was changed to when the package was imported. Thus, the original "Last Modified Time" is not preserved, which could cause issues with syncing TTL for active list entries across two systems.<br/> Now, a property has been added to the defaults.server.properties file to keep the Last Modified Time unchanged for entries in an active list imported from a package: entry.lastmodifiedtime.enabled=true
NGS-13299	Creation and last updated timestamps, and user IDs, were not preserved when case resources were imported. Now if the parameter "case.infonote.enabled" is set to "true" in the server.properties file, a note containing the original Creation Time, Last Modified Time, creator ID and modifier ID will be created for each case imported. Note: this will only be possible with packages created in 6.9.1 Patch 2 or later.
NGS-13261	Certain debug messages appear in logs. These messages have been turned off by default and can be turned on by editing <br/> net.sf.j2ep.ProxyFilter.level=FINE in<br/> /opt/arcsight/manager/arcsight-dm/logging.properties<br/>
NGS-12491	Importing XML cases archive format files from the archive/imports directory was not working. <br/> This issue is now fixed.
NGS-12341	By default, Instruments are not included in the Resource Validation Report. Customers now have to option to include them by adding the parameter includeTypes. For example: /opt/arcsight/manager/bin/arcsight resvalidate -includeTypes Instrument Note: Resources are case sensitive, therefore inputting "instrument" will not work.
NGS-11138	Channel with cases was not properly refreshed if it was opened in two Consoles by the same user. Data was refreshed only in one Console. Now, data in the channel is refreshed for all Consoles with any user.
NGS-9733	When logging in to the ArcSight Console, you could get an error related to logging in to core services. Login will still continue.
NGS-9080	In some cases, IP address geo location mappings returned incorrect results. The geo-location database has been updated, and now returns correct location information.

CORR-Engine

Issue	Description
NGS-21192	Manager Receipt Time field in the arc_event_annotation was not in sync with the event's actual Manager Receipt Time when events were annotated. The issue is now fixed.
NGS-21119	A signal 11 intermittently occurred in the MySQL storage engine. The issue is now fixed.
NGS-20319	When calculating space utilization, storage groups whose archive path was under another storage group archive path were counted twice. This is expected behavior. You should not nest storage groups. See the ArcSight Command Center Guide's topic on storage groups for more information.
NGS-19475	If the MySQL database password for user 'arcsight' contains a space character, the command /opt/arcsight/manager/bin/arcsight export_system_tables will not be able to connect to the database, and fail. This issue has been fixed for passwords with internal spaces. Passwords with leading and trailing spaces are not supported.
NGS-17406	The message "Logger server version is incompatible (should be 6.8.0.xxxx but is 6.8.0.yyyy)" was displayed in logger_web logs. The issue is now fixed.
NGS-16975	Capacity of Active List - "Storage Licensing Data by Connector" has been increased per customer request.
NGS-15465	Previously, if you moved a user to another group, created a link, and later, selected that user for deletion, the user would be deleted even if you did not confirm the deletion. Now, if you close the deletion confirmation popup window without confirming the deletion, the deletion action is canceled.

Command Center

Issue	Description
NGS-21982	When trying to access the Storage and Archive or other pages during a Command Center session, customers were getting session timeout intermittently. The issue is now fixed.
NGS-21583	Any pre-upgrade device custom ipv6 address data that is not in the right format of IPv4 or IPv6 addresses will not show up in the Command Center.

Issue	Description
NGS-20736	The dashboard page of ArcSight Command Center does not provide scrolling between tabs. To work around when the number of tabs causes dashboards tabs to be placed out of the window, adjust zoom level of the browser.
NGS-20484	In some cases, even with active user session ArcSight Command Center showed an error "Your session has timed out. Please login again" and redirected the user to the Login page. Mostly that was seen with such pages as Storage and Event Search. The problem is now fixed.
NGS-19961	If a new private Fieldset type is added to ArcSight Command Center, this Fieldset can only be used and edited by the author.
NGS-19510	AgentReceiptTime values were showing as epoch timestamps when events were exported from ArcSight Command Center to a CSV file.<br/> This issue has been fixed.
NGS-17474	When a case is viewed in ArcSight Command Center, renamed and saved, now when user go back to cases resource browser case are being displayed in grid. User has to refresh the grid.
NGS-17445	In certain publisher-subscriber configurations it was not possible to add a Peer configuration using Peer Authorization Credentials. This issue has been fixed.
NGS-16779	Some horizontal bar charts and moving average charts were not displayed correctly in ACC. <br/> This issue is now fixed.<br/>
NGS-16206	In the ArcSight Command Center, timestamps for stacked bar charts were ordered alphabetically rather than chronologically. This issue has been fixed.
NGS-14490	In an MSSP context, exporting search results using "Save to ArcSight Command Center" violates the separation between tenants within the system. To mitigate this by disabling the functionality, set search.export.saveToServer.enabled=false in logger.properties (as it is true by default/if absent).
NGS-14234	ArcSight Command Center did not allow fields within cases (including those within the events panel) to be copied and pasted into external handling tools. This issue is now fixed.
NGS-14169	When excluding Events in Search using alt-click, fields with null were also not included.<br/> A logger configuration "sqlgenerator.querystr.addnullcondition" can be added to enable the inclusion of the null value entries. The default value is false.

Issue	Description
NGS-13037	ArcSight Command Center results are now presented with a shaded background on alternating rows.
NGS-12968	The new date field global variable will not display date value correctly in ArcSight Command Center dashboards. For example, create a variable of this type : Type Conversion -> Convert String to Date WorkAround: Use this variable in two data monitors and add these data monitors to a dashboard. In the dashboard, one of the data monitor displays the date format correctly, but the other data monitor shows it as a long number.
NGS-7489	The session time out does not occur while the home page is loaded. If leaving a session unattended for an extended period, make sure you log out.

Connector Management

Issue	Description
NGS-13888	Previously, after going through the Connector import wizard, the configuration changes appeared for the Connector resource in the ArcSight Console, when viewed in the Inspect/Edit window. However, running agentsetup did not show that the changes had taken effect. Now, the Import Connector Configuration feature correctly updates the connector as well.

Installation and Upgrade

Issue	Description
NGS-21201	The HA installation updates the contents of the /root/.ssh directory on both the primary and the secondary. Before doing so, it copies this directory to /root/ssh.backup
NGS-20748	Duplicate entries in postgres users table could cause session timeouts and other issues. The upgrade process now checks for duplicated entries and automatically deletes duplicates as part of ESM upgrade.
NGS-19579	After upgrade from ESM6.8c to ESM6.9.1, notifications could result in an error "[base URL not configured, run managersetup]". Running managersetup would not resolve the problem. This condition has been fixed.
NGS-17370	The second and subsequent Connected Hosts entries were ignored by High Availability. This has been fixed.

Localization

Issue	Description
NGS-18487	The Japanese error message when a Console user selects a password that is too short was corrected.

NGS-16276	Localized date/time format: this note applies to ESM deployed in a localized environment. <br/>
	If the property report.datetime.dateFormat in server.properties is defined, ESM uses its value as the format string, otherwise it uses the standard java method to obtain localized date format: (DateFormat.getDateTimeInstance(DateFormat.SHORT, DateFormat.DEFAULT))<br/>
	The change affects only the report parameters - not report data (table columns)<br/>
	You can modify the following parameters in server.properties to configure data format for their report.<br/>
	# The date format for all report content<br/>
	report.content.dateFormat=dd MM yyyy HH:mm:ss<br/>
	# The date format for datetime report parameters (e.g. $CurrentDateTime, $Now)<br/>
	report.datetime.dateFormat=dd-MM-yyyy-HH:mm:ss<br/>
	# The date format for date report parameters (e.g. $CurrentDate)<br/>
	report.date.dateFormat=dd-MM-yyyy<br/>
	# The date format for month type report parameters (e.g. $CurrentMonth)<br/>
	report.month.dateFormat=MM-yyyy<br/>
	# The date format for week type report parameters (e.g. $CurrentWeek)<br/>
	report.week.dateFormat=ww-yyyy

Open Issues

This release contains the following open issues.

Analytics

Issue	Description
ESM-49283	When defining filters, for a hostname to be properly interpreted from the Request URL, the host name needs to be enclosed either within // (double slash) and / (single slash); or within // (double slash) and : (colon). For example: https://hostname.example.com:8443 Such an event is retrieved correctly with the 'Request Url Host Is Not Null' filter. Do not use a filter with a condition that says 'Request Url Host != Null' because != makes the filter invalid.
ESM-39405	If you create a report whose name contains Chinese characters, then send the report as a PDF attachment, the received email does not display the attachment's name correctly. The content of the report is correct; only the email attachment field is affected.
NGS-23500	HTML reports embedded in emails were not displaying Unicode Standard characters appropriately.
NGS-7181	Queries are very slow when they have a combination of aggregation, groupby, orderby, and a condition on a large active list or session list.

Analyze/Search

Issue	Description
NGS-8530	In the Command Center search feature, some expected fields are missing from exported search results. For example, search for events, click Export Results, and check All Fields in the page Export Options, then click Export and download the exported results. In these results, only some basic fields are listed, such as endTime, Name, sourceAddress, and others. Workaround: In the ACC search page, after a search is completed click Export. Instead of selecting the checkbox to include all fields, enter a comma-separated list of fields in the text area provided.

ArcSight Console

Issue	Description
NGS-23489	If two users each have a Console installed on the same Linux machine and they both try to upgrade to 6.11.0, the first upgrade will succeed but the second will fail with the error "/tmp/exportfile.pkcs12 (Permission denied)". Delete the file "/tmp/exportfile.pkcs12" and re-run consolesetup for the second user to transfer settings again.
NGS-23444	When ArcSight Console is in dark theme and you are running the "arcsight replayfilegen" command, then you will have difficulty following instructions on the Wizard. Workaround is to run the command while the Console is in the default theme.
NGS-23214	In FIPS mode, if you have used changepassword to encrypt either ssl.keystore.password or ssl.truststore.password, and then you run consolesetup, please check config/client.properties to make sure that you do not have entries for both ssl.keystore.password ssl.keystore.password.encrypted and likewise for ssl.truststore.password. If you do, please remove the entry that is not encrypted. If you do not do this, then the ESM console may not run properly.
NGS-23207	ArcSight Console will not work in FIPS mode if installed on Windows 7 Professional.
NGS-23198	The Console does not check Certificate Revocation Lists to determine if a CA-signed manager certificate has been revoked by the Certificate Authority.
NGS-23019	Print Spooler service needs to be running in Windows for Console to start.

Issue	Description
NGS-22947	Following are issues with ArcSight Console set to the dark theme. In certain areas, some issues are visual only and will not affect functionality. 1. The Print option in the Geographic Event Graph data monitor is NOT supported. 2. For the Last State data monitor added to the dashboard, configure and color chooser are NOT supported. 3. In Hierarchy Map data monitor added to dashboard, color chooser is disabled. 4. Use Case and Network Model Wizard are NOT supported. 5. Print rule definition option from the Rules resource tree will not be in dark theme. 6. Advanced options for circular layout of resource graph will not be in dark theme. 7. Hide Empty Triggers button shows font in white color after selection. This happens only in Windows Server 2012R2. 8. Mouse over on menu bar will not be in dark theme. 9. Drop down arrows in some dialogs will not be in dark theme.
NGS-22946	Dark theme on the Console have issues specific to Linux and MacOS: 1. Some Print options buttons will not be in Dark theme. 2. Folder icons on the resource tree are not entirely in Dark theme. 3. Manage hot keys buttons are not in Dark theme. 4. Some drop-down icons are not in Dark theme.
NGS-21831	InSubnet condition will now strictly enforce the use of the (*) wildcard. A filter like 10.10. will be marked as invalid.
NGS-19880	On Linux, mouse interaction with Console after maximizing may not respond as expected. Instead of maximizing, drag corners of Console to resize to fill desktop.
NGS-17864	On certain operating systems, show event details option on an eventID in a Query viewer does not show all event details like EventID, Start time, ManagerReceipt Time. Workaround: Open the event in an Active channel first and then view the event using Query viewer using Show Event Details. In some cases, restarting of the Console also solves the issue.
NGS-17863	In an MSSP environment, under certain circumstances a tenant may notice event(s) which should match the user group's Access Control List settings for Events, but these events will be stuck in "Loading Event..." state within the Active Channel. Workaround: Add the "Customer Name" column to the Active Channel and the events will load successfully.
NGS-15686	When using Logger Integration Commands, authentication on Logger 5.3 SP1 will fail when using password authentication. Workaround: Configure Logger and Integration Commands for one-time passwords.
NGS-15119	Entry's Creation Time value is not being displayed properly in Console.

Issue	Description
NGS-14227	In a Non-English installation in the Console, if you create a case and then immediately select Add to Case/Case in Editor, the events may not be added to the newly created case. Workaround: Save and lock the new case before adding events to it.
NGS-14002	If a report is run with a parameter on an annotation, the report result will be empty.
NGS-13829	Stages resources are erroneously not locked as system content and are editable from the ArcSight Console, on the resource Navigator > Stages resource tree. Do not customize or move these stages resources, as doing so might cause the Manager to become unusable. The system content stages are Closed, Final, Flagged as Similar, Follow-up, Initial, Monitoring, Queued, and Rule Created.
NGS-13475	Date values of custom parameters for Reports will display properly regardless of the format selected in preferences on the Console.
NGS-11278	When a non-admin user attempts to use an active channel filter to find cases using the Outcome After Research value in field = 'unauthorized activity', the active channel displays Loading resources in the name field, then changes to loading and hangs. In addition, the correct number of total cases is displayed in the upper right corner; however, the cases are not displayed in the channel.
NGS-11153	The Console starts up successfully, but with the error message "Cannot find sree properties in /home/arcsight/Console/current/reports/sree.properties." Workaround: Ignore this message.
NGS-8630	Not all drill-downs will be valid. A drill-down definition can be based on all available attributes, but when viewing a query viewer in a chart, not all attributes will be displayed. So a drill-down definition based on an attribute that is NOT part of a chart view will be invalid. In that case, the query viewer must be viewed in a table.
NGS-7173	The Console may become temporarily unresponsive for a few seconds when working with large active and session lists.
NGS-5981	When annotating groups of events, the count of events which the Console indicates were updated may not reflect the correct number of updated event records.
NGS-3084	Global variable fields of the type "GetActiveList" are not displayed on custom layouts and image dashboards. This behavior is seen on custom layouts when using the ArcSight Console, and image dashboards when using ArcSight Command Center. WorkAround: To view these fields correctly, use the standard layout on ArcSight Console.
NGS-1088	If a regular or inline filter with the condition "Event Annotation Flags Is NOT NULL" is applied to an active channel, the active channel will not load all of the matching events. Workaround: Use the following two filters in AND condition. EventAnnotationFlags Is NOT NULL EventAnnotationFlags != 0

ArcSight Manager

Issue	Description
ESM-51070	Connector statistics file to be processed correctly on Managers other than the primary destination Manager. Related content such as the rule Connector Discovered or Updated will be impacted.
ESM-48068	After asset auto-creation, if the Manager does not restart and the server.std.log shows a message about a "conflicting device with the same hostname/ipaddress <resource id>", then two assets have the same resourceId. This conflict has to be resolved before starting the Manager.
ESM-47625	When exporting a case or other resource, the Creation Time is changed to the time of the export.
ESM-46699	Updating a Trend by refreshing it works only once. Thereafter, the trend does not refresh with updated information.
ESM-30008	Installing an exported package from a bundle file occasionally results in the following error: Install Failed: Resource in broker is newer than modified resource. Workaround: Re-import the package.

Issue	Description
NGS-23503	If the Manager certificate is changed for any reason, such as an IP address change, hostname change, expired certificate, or IPv6 reconfiguration, the newly-generated Manager certificate must be imported on all clients as stated in the section "Changing the Hostname of Your Machine" in the ESM Installation Guide. But there are problems that may occur while attempting to replace a source Manager certificate on a Forwarding Connector. A deleted source Manager certificate may reappear in the Forwarding Connector truststore unless it is deleted from two separate truststores. Use the following procedure when the certificate of a source ESM Manager of a Forwarding Connector has changed: 1. Export the new Manager certificate from the source Manager. 2. Delete the old Manager certificate in the Forwarding Connector from both FIPS and non-FIPS truststores using the following sample commands. (Command samples are derived from the SmartConnector 7.5 User's Guide. The certificate alias and keystore password will vary based on your installation.) jre/bin/keytool -keystore jre/lib/security/cacerts -delete -storepass changeit -alias "hostname.yourdomain.net_8443-cn=hostname.yourdomain.net, ou=yourorg, o=acme, l=95014, st=ca, c=us-1490656465388" jre/bin/keytool -keystore user/agent/fips/bcfips_ks -storetype BCFKS -storepass change -delete -providername BCFIPS -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath lib/agent/fips/bc-fips-1.0.0.jar -J-Djava.security.egd=file:/dev/urandom -alias "hostname.yourdomain.net_8443-cn=hostname.yourdomain.net, ou=yourorg, o=acme, l=95014, st=ca, c=us-1490656465388" 3. Import the source Manager certificate into Forwarding Connector truststore (SmartConnector User Guide) 4. Runagent setup on Forwarding Connector to re-register the destination Managers to the connector. The full alias of the Manager certificate may be found by running the keytool command with the -list option using the following sample: jre/bin/keytool -keystore jre/lib/security/cacerts -list -storepass changeit
NGS-23341	If you see event broker connection up and down audit events continuously, it is likely that there is some issue with either the topic that the ESM is consuming from or the Event Broker that the ESM is connected too. Ensure that the Event Broker is healthy.
NGS-22470	In unusual cases the upgrade of the High Availability feature may report it was successful when it actually failed. Please run /usr/lib/arcsight/highavail/bin/arcsight_cluster status after an upgrade to be certain it really succeeded.

Issue	Description
NGS-14860	Multiple failure messages are generated in logger_web.out.log when stopping arcsight services. These messages can be ignored.
NGS-14437	In some cases when permission is not properly set or an account was improperly moved from a lower level to a higher level of ACL then an error message Not allowed to read 01000100010001001 (All Users) Error Messages in Logs
NGS-14383	Archive Processing Report lists don't differentiate Archive Name for different Storage Groups. Workaround: Use the FilePath field when working with Archive Audit Events.
NGS-14260	If some resource on the primary (for example, memory, or CPU) is temporarily exhausted, it may be necessary to reboot the primary to recover HA control completely. Symptoms during the resource exhaustion can include: 1. ESM running very slowly. 2. Cannot make a new SSH connection to the system. ESM will run normally after the resource exhaustion ends. But the following continuing symptoms may be seen: 1. HA will not failover via arcsight_cluster prefer or arcsight_cluster offline. 2. HA may report that the resources "ESM", "Filesystem", and "Service IP" are Stopped, when they evidently are running normally. If these symptoms are seen together, the primary system should be rebooted.
NGS-12358	A package resource may become out of sync with the content that has been added to the package. To workaround, recreate the package.
NGS-12105	The annotation stage name default value ('Queued') is displayed in the active channel, but this name does not display in the query viewer or in a report. Its other non-default value (for example, 'Initial', 'Follow-Up') is displayed correctly in the query viewer or report.
NGS-9734	In Russian, when a notification is sent with an email attachment, the filename and email subject lines contain garbled characters.
NGS-9109	An incorrect OID is provided for ArcSight SNMP Trap. A third party package causes the OID for a trap to be translated incorrectly.
NGS-8926	If there is a Forwarding Connector running between a source Manager and any destination, and a correlation event occurs on the source Manager, then the Forwarding Connector will forward the correlation event and its associated correlated events to the destination. However, the EventAnnotationFlags=correlated field will not be populated for the correlated events in the source Manager's database. As a result, if there is any correlation content on the source Manager looking for the value EventAnnotationFlags=correlated, the content will not be matched or triggered.

Issue	Description
NGS-3825	If the field size of an event exceeds 32 KB, that event does not persist.
NGS-1937	The Archive tool occasionally fails to import entries into an active list due to transient errors. In such situations, you might not see any errors, but the list is not populated. Workaround: Re-import the same package.
NGS-172	Base events are not automatically annotated after rules trigger. Workaround: Set logger.base-event-annotation.enabled=true in server.properties.

CORR-Engine

Issue	Description
NGS-14477	Space-based retention cleans up same day data, but even after increasing the space, the system does not recognize that the space has been increased until midnight.
NGS-14041	Database queries using the UPPER or LOWER built-in string functions in the Russian locale return incorrect results when filtering events. This applies especially to queries using the "Ignore Case" option, which rely on the UPPER function.
NGS-11080	When offline event archives are restored to another system using the restorearchives command, the event annotations are not restored. The offline archives are not affected.
NGS-9503	There is a possibility that small segments of data in the CORR-Engine may become corrupted. If a query attempts to access data that has become corrupted, the query will skip the corrupted data and log an error message in the MySQL log. This enables MySQL to continue and return a result on the data that is not corrupted.
NGS-4837	With certain long running queries, a deadlock might occur in the JDBC driver. You might notice decreased throughput. If you suspect this, request a thread dump through manage.jsp and determine if the end of the dump specifically indicates "deadlock." Workaround: If a deadlock does occur and is an issue for you, restart the Manager to resume normal operations.
NGS-4790	To resolve a "database full" condition, free up space in the ArcSight System Storage Space by doing the following: 1. Delete any unused trends. Deleting the trend frees up any data in the table associated with this trend. 2. Reduce the retention period of specific trends. By default, trends retain 180 days of data. You can set this retention time on a per-trend basis. Any data falling outside this range will be removed the next time the trend runs. 3. Examine the contents of your session lists. Data is not usually removed from session lists. Running "bin/arcsight dropSLPartitions -h" will explain how to remove data older than a specified time. Note that this will apply to ALL session lists on your system.

Command Center

Issue	Description
NGS-23560	In Event Search, when searching events from Logger peers and the search query contains "by name span (endTime)=", the search might be disrupted and a NullPointerException error message will be displayed in the Event Search page. This only happens to certain types of data.
NGS-23549	The Tools dialog goes at the top of the screen at the point where it looks cut off, when you are selecting the first 5 row options of the grid. This happens when IPAddress value is IPv6.
NGS-23437	If you set a background image to a dashboard using the ArcSight Console, this image is NOT set to the same dashboard when viewed in the ArcSight Command Center.

NGS-23429	Reports run as HTML format from ArcSight Command Center containing charts do not show up in the report output when the server is configure with below properties. The properties are to save report output in database. Workaround is to run in pdf.
	vfs.report.provider.scheme=db
	vfs.report.provider.class=com.arcsight.common.vfs.database.ArcDatabaseFileProvider
	vfs.report.provider.base=db://reports/archive

NGS-23137	OTP session for Logger integration command doesn't work the first time, but works fine next time till session is on.
NGS-23105	If the manager has a CA signed certificate where the certificate is signed with the SHA1 algorithm, Command Center may not work on IE or Chrome browsers. CA signed certificates signed with SHA256 or SHA384 do not have these problems, and are recommended.
NGS-22583	"Condition Summary" is not formatted in color codes and also does not display the field's "Display Name", when a drilldown is created based on active channel.
NGS-22573	The ArcSight Command Center User's Guide states that FIPS Suite B Mode is not supported for peering or content management. The Administration->Content Management and Administration->Peers menu items are disabled if the server is running in FIPS Suite B mode. However, the aforementioned menus are enabled if the manager from which you initiate peering is not in FIPS Suite B mode, even if the target of the peer relationship is in FIPS Suite B mode. This is still an unsupported configuration. But Command Center does not have visibility into the FIPS mode of the target manager so it cannot disable the menu item. To repeat, peering and content management are not supported if either manager in the peer relationship is in FIPS Suite B mode.
NGS-22566	If scrollbars are missing in Safari browsers, please do the following: 1. Launch "System Preferences" from the "Apple menu" 2. Click on the "General" settings option 3. Look for 'Show scroll bars' and select the radio box next to "Always"

Issue	Description
NGS-22085	In the ArcSight Command Center, for Query viewers, Stacked Bar chart will not be supported if Y axis or Z-axis is not aggregated fields. In such cases user has to view in Table format.
NGS-21986	Viewing Last N events Data Monitor in Command Center containing too many Variable fields based on overlapping Session List may cause Java Script unresponsive error. Workaround: Limit the data monitor to six variiable fields with 10 rows, or split the fields by creating one or more data monitors.
NGS-21227	After correcting and validating a channel filter condition, the Channel Editor dialog still indicates that the filter is invalid. This may be ignored, and the Update button may be selected to update the filter.
NGS-20458	The search parameter | regex "#" will cause the search query to fail and will throw a 503 service request error. Once the page gets a 503 error, it does not leave this state. Refresh the page (press F5).
NGS-20280	The WHERE operator is not supported in user-defined fields.
NGS-19267	It was not possible to restrict access to cases by user in Command Center. A new property has been created to allow this. In order to enable the functionality, set "restrict.access.to.cases" to "true" in the server.properties file, then use "Edit Access Control" in ArcSight Console. Existing cases will not be affected.
NGS-17407	If the system has too many notifications, Command Center will not show notification counts in notification view. Workaround: Stop Manager, delete unused notifications such as undeliverable or old pending notifications, and start Manager.
NGS-14900	There is a rare case that may cause confusion in channel event data visualization screen, if the event interval is less than 1 minute apart. The depending charting library, d3.js, is not able to handle this minute rounding case. The issue will rarely occur in a production environment.
NGS-13926	The stages available in the ArcSight Console Stage drop-down list do not always display in the Command Center active channel. The stage "Follow-Up" is available in the ArcSight Console Annotation Stage drop-down list, but does not display in the Annotation Stage drop-down list in Command Center active channel.
NGS-13854	If you are using other than an English installation, some dashboard pages may not load in the Command Center. You can still access these pages through the ArcSight Console.
NGS-7912	In peer search, the search result is not refreshed responsively if one peer node has high hits, or the system is busy due to high ingestion rate or multiple searches running.
NGS-7907	When you perform peer search using IN operators for IP address, MAC address, or Enum fields, no results are returned and an error message is displayed.

Issue	Description
NGS-7891	In Command Center Search, queries using some operators, such as chart, eval, rename, replace, rex, and regex, may not return the correct results when searching the following types of fields. IPv4 fields such as sourceAddress, MAC address fields such as destinationMacAddress, IPv6 fields such as dvc_custom_ipv6_address1, Geo Location fields such as: dest_geo_latitude, as well as the agentSeverity and locality fields. For example the following queries may not return the correct results: ... | chart max(agentSeverity) by name ... | chart max(dest_geo_longitude) by name ... | replace Low with notToWorry in agentSeverity ... | replace Local with localevents in locality
NGS-7594	In the ArcSight Command Center, if you search by Load a Save Search filter, when the session times out, if you click the "Save current search filter" icon or "Load a save search filter" icon, you get logged out without a way to log back in. Workaround: When you see this behavior, close the browser window, reopen it, and log in to ArcSight Command Center again and continue with the search.
NGS-7584	A condition in a case query group with owner = <username> will return an error while viewing cases of a case query group in any UI. Workaround: Use owner = <user resource_id> instead of owner = username.
NGS-7518	In a Safari browser on a Mac OS, the search results page my not include a horizontal scroll bar. Workaround: Resize the browser to get the horizontal scroll bar.
NGS-6886	When a system has several peers and a peer stops responding, some pages in the ArcSight Command Center user interface might become slow to display. The delay happens regardless of the reason the peer system stopped responding. Workaround: Identify the peer that is not responding and remove its peer relationship on the Administration > Peers page, Peer Configuration tab. You can re-add the peer later, when it is back in service.
NGS-6812	The ESM server log and the Logger server log may contain messages that say "...NotSerializableException: ...PeerLoggerRequestDestination". These messages do not indicate an active problem, and can be ignored.
NGS-6805	When using the Chrome browser, the drop down to edit the Notification State or Storage Mapping might remain displayed when you move somewhere else by clicking outside the drop-down. Workaround: Click inside the drop-down and then click outside of it again to cause it to be removed from display.

Connector Management

Issue	Description
NGS-22669	When events are sent to ESM via an Event Broker, payload information cannot be retrieved for the corresponding event.

Connectors

Issue	Description
NGS-23179	Command "./arcsight agent tempca -i" in Connector 7.5.0.7983.0 with SuiteB mode will throw an exception. Update connector to a version later than version 7.5 where this might be addressed.
NGS-13049	When upgrading the Forwarding Connector, two fatal exception messages will appear, regarding [agents[0].arcsightuser] and [agents[0].arcsightpassword]. These messages may be safely ignored.
NGS-12407	Annotation flag indicating 'forwarded' may not get set when forwarding events from ESM 6.8.
NGS-1423	Upgrading a connector running on Windows from the ArcSight Console will fail if any process is using the connector's "current" folder. Workaround: 1. Make sure there are no files in the connector's "current" folder open. 2. Start the connector by using Start > Programs > Connector Programs. Do not start the connectors using the "arcsight agents" command.

General

Issue	Description
NGS-23640	ArcSight Investigate searches on the Severity field may not work in some cases as ESM enhances the value received from the connector, and the value may not be same in ESM as in ArcSight Investigate.
NGS-23639	When you invoke Investigate from ESM on string based fields containing leading or trailing spaces, the search will fail. In such cases, manually fix spaces before/after the value because of the differences in ESM and ArcSight Investigate storage.

Issue	Description
NGS-23563	Content based ArcSight investigate command is launched containing values with special characters such as the ampersand (&amp;), enclose the values in single quotes in ArcSight investigate search query before executing the search.
NGS-23554	After launching Arcsight Investigate integration command on integer fields such as source port, change the search condition value to 0,NONE.
NGS-23464	During Event Broker connector upgrade process from ESM, the icon is switched back to the normal icon even when the connector still has the Event Broker destination and won't change back to the Event Broker Icon until it is restarted.

Installation and Upgrade

Issue	Description
NGS-23201	After an upgrade of a FIPS installation, utilities on the manager machine that log into the manager (e.g. arcsight archive) may not work. To get these utilities to work, do the following steps: 1. Add the following lines to /opt/arcsight/manager/config/client.properties, creating the file if it does not exist: ssl.keystore.type=BCFKS ssl.keystore.path=config/keystore.client.bcfks ssl.truststore.type=BCFKS ssl.truststore.path=config/keystore.client.bcfks 2. Export the manager certificate: /opt/arcsight/manager/bin/arcsight keytool -store managerkeys -exportcert -alias mykey -file manager.cer 3. Import the manager certificate into the client truststore /opt/arcsight/manager/bin/arcsight keytool -store clientcerts -importcert -alias mykey -file manager.cer
NGS-21995	Resource validators for IP Address data have been tightened. On upgrade, any resource containing incorrect IP Addresses or IP Ranges will be invalidated and the conditions may be cleared. Rebuild the invalidated resource after upgrade.

Issue	Description
NGS-21133	During ESM upgrade, if the fully qualified domain name (FQDN) does not resolve to the IP Address of the ESM host, the upgrade process might freeze and fail eventually. If this is the case, check the upgrade log file /opt/arcsight/logger/current/arcsight/logger/logs/logger_init_driver.log if it contains this message: "Starting Apache...httpd: Could not open configuration file /opt/arcsight/logger/current/local/apache/conf/httpd.conf: No such file or directory Failed to start. Stopping APS...APS was not running." To prevent this failure, make sure FQDN is configured properly on ESM host before starting upgrade process.
NGS-19862	Before ESM installation, please make sure the system has a configured hostname that resolves to a local IP address.
NGS-14188	ESM Console installation on non-English path in Windows machines fails to configure Console. Workaround: Use English filenames in installation paths. Or run Console configuration after installation finished by running the consolesetup script from Console ..\current\bin directory.
NGS-7497	Console installation on localized path is working in some Windows 7 machines when installed in a French name like "C:\d'enqu&#xEA;te" but not in other Windows 7 machines. Workaround: Due to the inconsistent behavior in Windows 7 machines, use English filenames only in installation paths. French names in paths may cause installation to fail in certain Windows 7 environments.
NGS-6996	There might be some data monitors disabled after the upgrade, while they are enabled in a fresh installation and vice versa. Workaround: Re-enable any data monitors that you want enabled after upgrade.
NGS-3839	Occasionally, the First Boot Wizard may fail to proceed due to some errors. If this happens, terminate the process. After checking the logs and correcting the errors, follow the clean up instruction in the ESM Installation Guide and re-launch the installer.
NGS-3322	Due to the timing of some components' start-up, there may be some harmless error messages in the log files such as: [FATAL][default.com.arcsight.logger.distributed.DirectConnection$ReadChannel][run] java.io.IOException: end of communication channel [FATAL][default.com.arcsight.logger.distributed.ClientDirectConnection][run] java.nio.channels.ClosedChannelException
NGS-2783	When a Forwarding Connector is installed, Superconnectors group is created under Custom Users Groups group. In addition, No Events enforcing filter is replaced by a specific event filter. After the upgrade, No Events enforcing filter will be reinstated meaning that no events will be forwarded from the Manager to the destination. Workaround: Remove the No Events enforcing filter.

Localization

Issue	Description
NGS-23004	On a system with the Simplified Chinese locale, after import one case package that is created in English locale, the properties of the case may have default values instead of the entered values. This issue exists in both ArcSight Command Center and ArcSight Console."
NGS-22991	In Simplified Chinese and Traditional Chinese, if you create a data monitor with the type HourlyCount and view it as Tile, its display will hang - no data will be displayed.
NGS-22600	On a Traditional Chinese Installation, when you display the "Top Value Count" dashboard, the Stacking Area, Area,Scatter Plot, and Line options show no data. The Bar, Pie, and Stacking Bar options do display data.
NGS-22568	In Traditional Chinese the function LengthOf may display incorrect values and/or produce the wrong filter results.
NGS-21872	If you retrieve logs via the Command Center on an ESM localized to other than English, the Command Center will not inform you when the logs have been retrieved. Workaround: Refer to the log retrieval page. You will find your newly generated logs.
NGS-14191	When you run the Database Performance Statistics dashboard in an environment that has a local language other than English, you may see two sets of entries in the Database Free Space area: one in the local language used by ESM, and the other in English. If this happens, both the ArcSight Console and the ArcSight Command Center will be affected.

NGS-10687	If the property (report.datetime.dateFormat) in server.properties is defined, the value is used as the format string. Otherwise, standard Java is used to get the localized date format (DateFormat.getDateTimeInstance(DateFormat.SHORT, DateFormat.DEFAULT)).
	The change affects only the report parameters - not report data (table columns).
	User can modify the followings in server.properties to configure data format for their report.
	# The date format for all report content
	report.content.dateFormat=dd MM yyyy HH:mm:ss
	# The date format for datetime report parameters (e.g. $CurrentDateTime, $Now)
	report.datetime.dateFormat=dd-MM-yyyy-HH:mm:ss
	# The date format for date report parameters (e.g. $CurrentDate)
	report.date.dateFormat=dd-MM-yyyy
	# The date format for month type report parameters (e.g. $CurrentMonth)
	report.month.dateFormat=MM-yyyy
	# The date format for week type report parameters (e.g. $CurrentWeek)
	report.week.dateFormat=ww-yyyy

Reports

Issue	Description
NGS-20509	Peer reports fail when Logger is peered with ESM 6.8c and onwards. This happens because the database type of the event field "arc_sourceAddress" is different for Logger and ESM. Workaround: None available at this time.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Release Notes (ESM 6.11.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!